AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	Case No. 1:19-SW-1609
13109 PENNYPACKER LANE, FAIRFAX, VIRGINIA 22033 (SUBJECT PREMISES #1)	)	**UNDER SEAL**

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before December 20, 2019 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to The Honorable Ivan D. Davis *(United States Magistrate Judge)*.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____

Date and time issued: 6 Dec 19 @ 1503 hrs

/s/
Ivan D. Davis
United States Magistrate Judge
Judge's signature

IDD 12/23/2020

City and state: Alexandria, Virginia

The Honorable Ivan D. Davis, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
1:19-SW-1609	12/9/19 6 AM	N/A

Inventory made in the presence of :
N/A

Inventory of the property taken and name of any person(s) seized:
See attached, two pages FD-597

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 12/23/19

Executing officer's signature

D A Mockenhaupt FBI SA

Printed name and title

FD-597 (Rev. 4-13-2015)

UNITED STATES DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

RECEIPT FOR PROPERTY

Case ID: 281W-WF-3161747

On (date) 12/9/2019 item(s) listed below were:

- ☒ Collected/Seized
- ☐ Received From
- ☐ Returned To
- ☐ Released To

(Name) Tyler Pham

(Street Address) 13109 Pennypacker Ln

(City) Fairfax, VA

Description of Item(s):

Item #	Description **
1	Black magazine for handgun
2	Ammunition for 9mm handgun
3	Black iPhone
4	Pink iPhone
5	Ammunition for 9mm handgun
6	Black Asus notebook PC FX502V S/N H6N0CV15L084260 and power cord
7	Silver magazine for 9mm handgun
8	Ammunition for 9mm handgun
9	Ammunition for 9mm handgun
10	Black Mylar packaging - containing multi colored pills
11	Ammunition for 9mm handgun
12	Digital scale
13	Black magazine and 9mm handgun #0707447
14	Silver magazine and black/silver 9mm handgun #906116
15	Ammunition for shotgun 12 gauge
16	Ammunition for 9mm handgun
17	Dell inspiron 14 5000 laptop #G6RXGT2
18	Apple MacBook Air A7932 S/N FVFYN4588147C
19	Alarm Clock/Camera
20	Black Hewlett Packard Elitebook 840 laptop
21	12 gauge ammunition
22	9mm ammunition Sig Sauer
23	870 black shotgun W530363M, 12 gauge
24	Financial documents
25	2 passports
26	Letter from DEA
27	Financial documents

UNITED STATES DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

RECEIPT FOR PROPERTY

28	Financial documents
29	Financial documents
30	Financial documents
31	iPhone in pink case
32	Resealable bags
33	Thumb drives
34	Digital scale
35	Hard drives and thumb drives
36	Financial documents
37	USPS receipt package to Arlington, TX
38	Pink laptop bag
39	Financial documents
40	12 gauge ammunition
41	12 gauge ammunition
42	Money counter
43	$936
44	$217
45	BBT Home equity line statement
46	Chase bank credit card statement
47	$390
48	$1805
49	$460
50	$3251

Received By: Left at Residence (signature)

Received From: [signature] (signature)

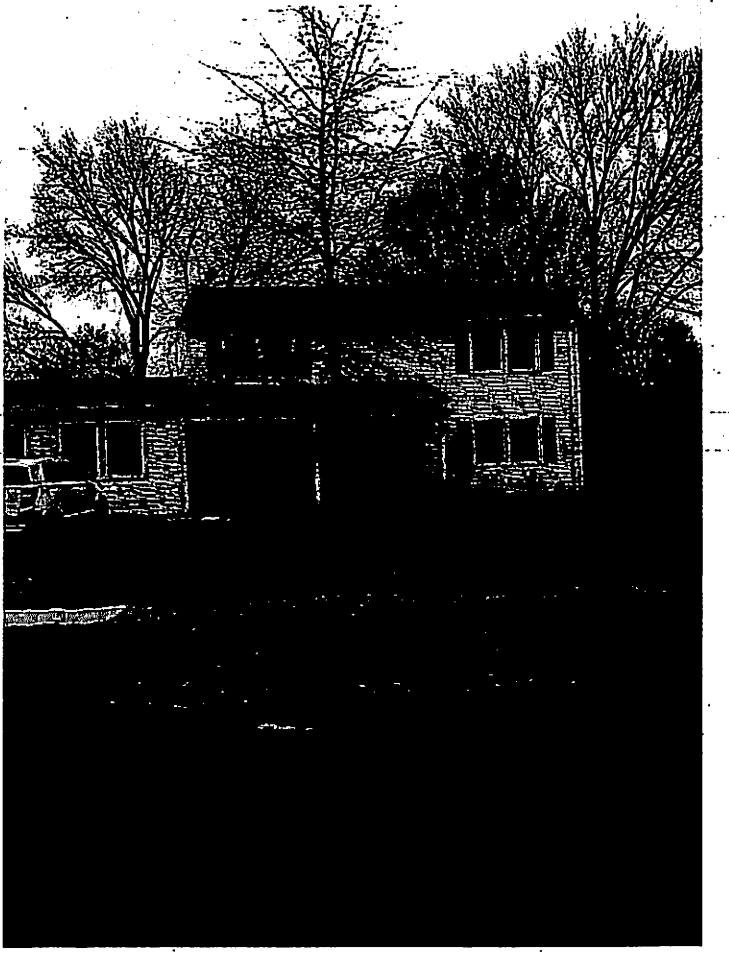
Printed Name/Title: Left at Residence

Printed Name/Title: Dwayne Thompson / Special Agent

ATTACHMENT A-1

Property to be Searched

The premises to be searched is the following, including any and all structures and/or vehicles located within the curtilage thereof: 13109 Pennypacker Lane, Fairfax, Virginia 22033, within the county of Fairfax. The nearest cross street is Pageant Lane. The property is a multi-level single family home. There is an overhang over the front door and the numbers "13109" are displayed horizontally on the overhang and above the front door. The overhang is supported by white pillars. The structure consists of yellow siding and it has white window frames with brown shutters. The driveway is to the left of the front door but there is no garage at the end of the driveway.



ATTACHMENT B

Property to be Seized

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841, 843 and 846 (distribution and possession with intent to distribute, and conspiracy to distribute and possess with intent to distribute, controlled substances, including by means of the Internet, and illegal use of the mail):

a. Controlled substances, in particular Adderall and methamphetamine;

b. Items commonly associated with the packaging and sales of controlled substances, including USPS packaging, sealed parcels prepared for mailing, gray and manila bubble mailers, address labels, black foil bags, raisin boxes, plastic bags or zip lock bags;

c. Photographs and/or video, in particular photographs and/or videotapes of potential co-conspirators and their criminal associates, assets, and/or controlled substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators;

d. Records, correspondence, narcotic customers lists, narcotic suppliers lists, ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts, letters and memoranda of agreements between potential coconspirators, formulas, receipts, phone records, phone books, address books, notations and other papers, and any files relating to the transporting, ordering, purchasing, or distributing of controlled substances;

e. Records relating to the use of and accumulation of proceeds derived from the sale of Adderall and methamphetamine or any other illegal controlled substances, as well as the acquisition of property obtained from drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money obtained from drug sales, including records of large purchases, receipts, canceled checks, bank records, credit card records, wire transfers, wire transfer receipts, cashier's checks, cashier's check receipts, addressed mail, express delivery receipts/envelopes, utility company receipts, rent receipts, income tax returns, money drafts, money orders, and their receipts;

f. Financial records including expenses incurred in obtaining the equipment and items necessary for the transportation and/or distribution of controlled substances, income derived from the sales of controlled substances, as well as records of legitimate income or lack thereof, and general living expenses;

g. United States currency in excess of $1,000, cryptocurrency also known as virtual currency, including bitcoin, stored on electronic or paper wallets or other means, cryptocurrency private keys and recovery seeds, gift cards, cash cards, and records relating to income derived from the transportation, sales, and distribution of controlled

substances and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, checkbooks, check registers, securities, precious metals, jewelry, antique or modern automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of illicit controlled substances trafficking;

h. Documents indicating travel in interstate and foreign commerce, such as travel itineraries, plane tickets, boarding passes, motel and hotel receipts, passports and visas, credit card receipts, and telephone bills;

i. Receipts, notes, ledgers, records, programs, and applications relating to Bitcoin and other cryptocurrencies;

j. Records reflecting names, addresses, telephone numbers, internet monikers, and other contact or identification data for others involved in the exchange of bitcoin and other cryptocurrencies;

k. Any digital device used to facilitate the above listed violations and forensic copies thereof;

l. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the categories of items to be seized described herein:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the use of virtual private networks and the TOR network including, but not limited to, access of darknet marketplaces;

iv. evidence of the attachment of other devices;

v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

vi. evidence of the times the device was used;

vii. passwords, encryption keys, PGP keys, recovery seeds, and other access devices that may be necessary to access devices;

viii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

ix. records of or information about Internet Protocol addresses used by the device; and

x. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Any and all cryptocurrency, to include the following:

i. any and all representations of cryptocurrency public keys or addresses, whether in electronic or physical format;

ii. any and all representations of cryptocurrency private keys, whether in electronic or physical format;

iii. any and all representations of cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include "recovery seeds" or "root keys" which may be used to regenerate a wallet.

n. The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States.

n. The United States is further authorized to copy any wallet files and restore them onto computers controlled by the United States. By restoring the wallets on its own computers, the United States will continue to collect cryptocurrency transferred into the wallets seized as a result of transactions that were not yet completed at the time that the devices were seized.

2. As used herein, the terms "records," "documents," "programs," "applications," "materials," and "information" include all forms of creation or storage, including in digital form on any digital device and any forensic copies thereof as well as any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

3. As used herein, the term "computer" is an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in

conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

4. As used herein, the term "storage medium" includes any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

6. For any computer or storage medium whose seizure is otherwise authorized by the search warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER").

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the use of virtual private networks and the TOR network including, but not limited to, access of darknet marketplaces;

f. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

g. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

h. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

i. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

j. evidence of the times the COMPUTER was used;

k. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

l. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

m. records of or information about Internet Protocol addresses used by the COMPUTER;

n. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

o. Routers, modems, and network equipment used to connect COMPUTERs to the Internet; and

p. contextual information necessary to understand the evidence described in this Attachment B.

7. During the execution of the search of the **SUBJECT PROPERTIES** described in Attachments A-1, A-2, and A-3, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the **SUBJECT PROPERTIES** to the Touch ID sensor of any Apple brand device(s), such as an iPhone or iPad, found at the **SUBJECT PROPERTIES** and to hold the digital devices found at the **SUBJECT PROPERTIES** in front of the face of individuals found at or in the **SUBJECT PROPERTIES** with the individuals' eyes open to activate the facial-, iris-, and/or retina-recognition features for the purpose of attempting to unlock the device via Touch ID, Face ID or similar biometric features in order to search the contents as authorized by this warrant.

8. The search warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate

evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

9. Any locked container such as a safe may be searched for the property to be seized set forth herein;

10. If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do *not* involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (*e.g.*, the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team. This investigation is presently covert and the government believes that the subject(s) of the search is not aware of this warrant.